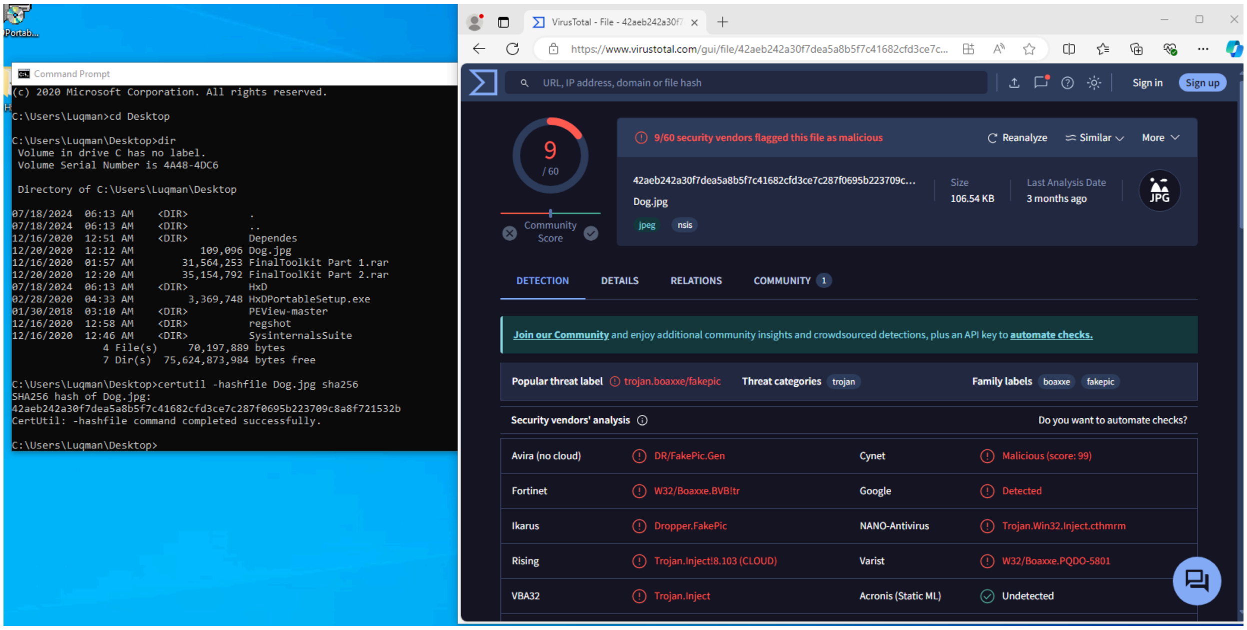
SIEM & SOC - FINAL PROJECT part 2

We are conducting a security analysis of the file "dog.jpg" to assess its potential malicious content.

I generated a hash from the file and checked it on VirusTotal.



```
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Luqman>cd Desktop

C:\Users\Luqman\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 4A48-4DC6

 Directory of C:\Users\Luqman\Desktop

07/18/2024  06:13 AM    <DIR>          .
07/18/2024  06:13 AM    <DIR>          ..
12/16/2020  12:51 AM    <DIR>          Dependes
12/20/2020  12:12 AM           109,096 Dog.jpg
12/16/2020  01:57 AM        31,564,253 FinalToolkit Part 1.rar
12/20/2020  12:20 AM        35,154,792 FinalToolKit Part 2.rar
07/18/2024  06:13 AM    <DIR>          HxD
02/28/2020  04:33 AM         3,369,748 HxDPortableSetup.exe
01/30/2018  03:10 AM    <DIR>          PEView-master
12/16/2020  12:58 AM    <DIR>          regshot
12/16/2020  12:46 AM    <DIR>          SysinternalsSuite
               4 File(s)     70,197,889 bytes
               7 Dir(s)  75,624,873,984 bytes free

C:\Users\Luqman\Desktop>certutil -hashfile Dog.jpg sha256
SHA256 hash of Dog.jpg:
42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b
CertUtil: -hashfile command completed successfully.

C:\Users\Luqman\Desktop>
```

VirusTotal - File - 42aeb242a30f7
https://www.virustotal.com/gui/file/42aeb242a30f7dea5a8b5f7c41682cfd3ce7c...
URL, IP address, domain or file hash
Sign in
Sign up
9
/ 60
Community Score
Reanalyze
Similar
More
JPG
DETECTION
DETAILS
RELATIONS
COMMUNITY 1

9/60 security vendors flagged this file as malicious

42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c...
Dog.jpg
jpeg nsis

Size 106.54 KB
Last Analysis Date 3 months ago

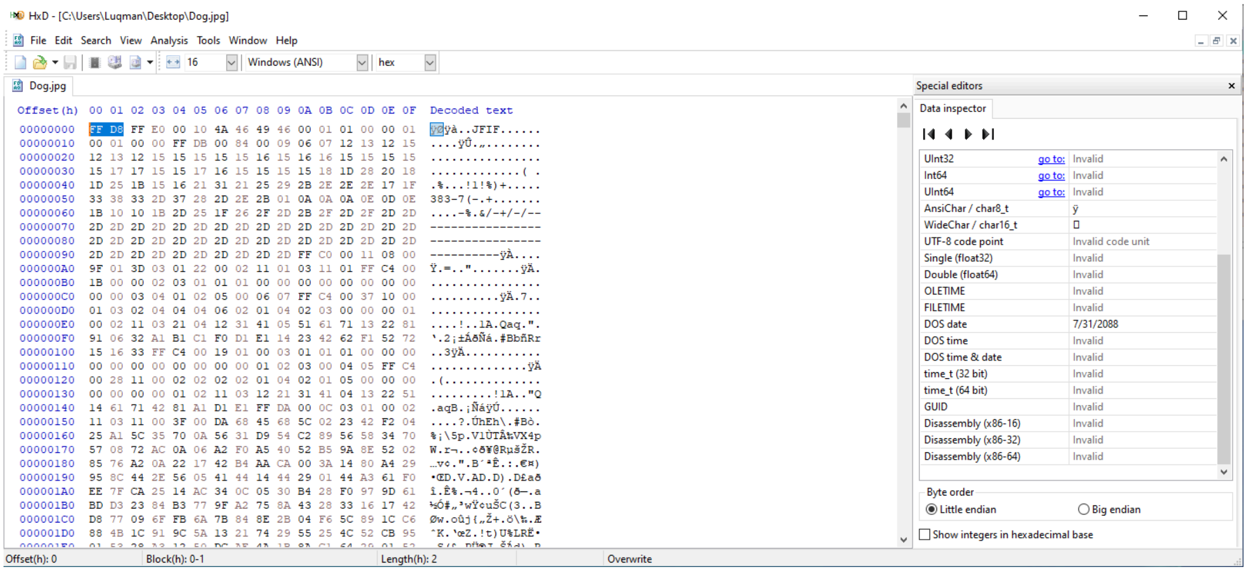
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.boaxxe/fakepic Threat categories trojan Family labels boaxxe fakepic

Security vendors' analysis   Do you want to automate checks?

Avira (no cloud)	DR/FakePic.Gen	Cynet	Malicious (score: 99)
Fortinet	W32/Boaxxe.BVB!tr	Google	Detected
Ikarus	Dropper.FakePic	NANO-Antivirus	Trojan.Win32.Inject.cthmrm
Rising	Trojan.Inject!8.103 (CLOUD)	Varist	W32/Boaxxe.PQDO-5801
VBA32	Trojan.Inject	Acronis (Static ML)	✓ Undetected

A JPG file in hexadecimal notation should start with the specific sequence FFD8 and end with FFD9. I checked the file in HxD and discovered that there is a significant portion of data appended after the FFD9 marker.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ÿØÿà..JFIF......
00000010  00 01 00 00 FF DB 00 84 00 09 06 07 12 13 12 15  ....ÿÛ.„........
00000020  12 13 12 15 15 15 15 15 16 15 16 16 15 15 15 15  ................
00000030  15 17 17 15 15 17 16 15 15 15 15 18 1D 28 20 18  .............( .
00000040  1D 25 1B 15 16 21 31 21 25 29 2B 2E 2E 2E 17 1F  .%...!1!%)+.....
00000050  33 38 33 2D 37 28 2D 2E 2B 01 0A 0A 0A 0E 0D 0E  383-7(-.+.......
00000060  1B 10 10 1B 2D 25 1F 26 2F 2D 2B 2F 2D 2F 2D 2D  ....-%.&/-+/-/--
00000070  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D  ----------------
00000080  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D  ----------------
00000090  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D FF C0 00 11 08 00  ----------ÿÀ....
000000A0  9F 01 3D 03 01 22 00 02 11 01 03 11 01 FF C4 00  Ÿ.=.."......ÿÄ.
000000B0  1B 00 00 02 03 01 01 01 00 00 00 00 00 00 00 00  ................
000000C0  00 00 03 04 01 02 05 00 06 07 FF C4 00 37 10 00  ..........ÿÄ.7..
000000D0  01 03 02 04 04 04 06 02 01 04 02 03 00 00 00 01  ................
000000E0  00 02 11 03 21 04 12 31 41 05 51 61 71 13 22 81  ....!..1A.Qaq.".
000000F0  91 06 32 A1 B1 C1 F0 D1 E1 14 23 42 62 F1 52 72  '.2¡±ÁðÑá.#BbñRr
00000100  15 16 33 FF C4 00 19 01 00 03 01 01 01 00 00 00  ..3ÿÄ...........
00000110  00 00 00 00 00 00 00 00 01 02 03 00 04 05 FF C4  ..............ÿÄ
00000120  00 28 11 00 02 02 02 02 01 04 02 01 05 00 00 00  .(..............
00000130  00 00 00 00 01 02 11 03 12 21 31 41 04 13 22 51  .........!1A.."Q
00000140  14 61 71 42 81 A1 D1 E1 FF DA 00 0C 03 01 00 02  .aqB.¡ÑáÿÚ......
00000150  11 03 11 00 3F 00 DA 68 45 68 5C 02 23 42 F2 04  ....?.ÚhEh\.#Bò.
00000160  25 A1 5C 35 70 0A 56 31 D9 54 C2 89 56 58 34 70  %¡\5p.V1ÙTÂ‰VX4p
00000170  57 08 72 AC 0A 06 A2 F0 A5 40 52 B5 9A 8E 52 02  W.r¬..¢ð¥@RµšŽR.
00000180  85 76 A2 0A 22 17 42 B4 AA CA 00 3A 14 80 A4 29  …v¢.".B´ªÊ.:.€¤)
00000190  95 8C 44 2E 56 05 41 44 14 44 29 01 44 A3 61 F0  •ŒD.V.AD.D).D£að
000001A0  EE 7F CA 25 14 AC 34 0C 05 30 B4 28 F0 97 9D 61  î.Ê%.¬4..0´(ð—.a
000001B0  BD D3 23 84 B3 77 9F A2 75 8A 43 28 33 16 17 42  ½Ó#„³wŸ¢uŠC(3..B
000001C0  D8 77 09 6F FB 6A 7B 84 8E 2B 04 F6 5C 89 1C C6  Øw.oûj{„Ž+.ö\‰.Æ
000001D0  88 4B 1C 91 9C 5A 13 21 74 29 55 25 4C 52 CB 95  ˆK.'œZ.!t)U%LRË•
```

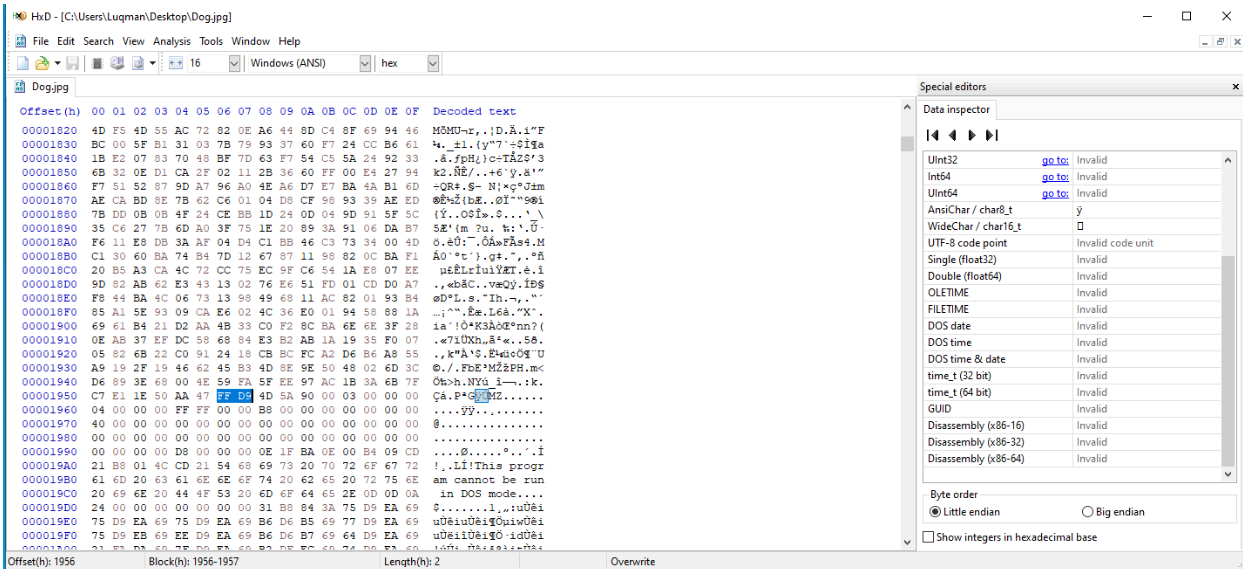
UInt32	go to:	Invalid
Int64	go to:	Invalid
UInt64	go to:	Invalid
AnsiChar / char8_t		ÿ
WideChar / char16_t		▯
UTF-8 code point		Invalid code unit
Single (float32)		Invalid
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		7/31/2088
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid
time_t (64 bit)		Invalid
GUID		Invalid
Disassembly (x86-16)		Invalid
Disassembly (x86-32)		Invalid
Disassembly (x86-64)		Invalid

Byte order

● Little endian ○ Big endian

□ Show integers in hexadecimal base

Offset(h): 0 Block(h): 0-1 Length(h): 2 Overwrite



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00001820  4D F5 4D 55 AC 72 82 0E A6 44 8D C4 8F 69 94 46  MõMU¬r,.¦D.Ä.i”F
00001830  BC 00 5F B1 31 03 7B 79 93 37 60 F7 24 CC B6 61  ¼._±1.{y“7`÷$Ì¶a
00001840  1B E2 07 83 70 48 BF 7D 63 F7 54 C5 5A 24 92 33  .â.ƒpH¿}c÷TÅZ$’3
00001850  6B 32 0E D1 CA 2F 02 11 2B 36 60 FF 00 E4 27 94  k2.ÑÊ/..+6`ÿ.ä'”
00001860  F7 51 52 87 9D A7 96 A0 4E A6 D7 E7 BA 4A B1 6D  ÷QR‡.§– N¦×çºJ±m
00001870  AE CA BD 8E 7B 62 C6 01 04 D8 CF 98 93 39 AE ED  ®Ê½Ž{bÆ..ØÏ˜“9®í
00001880  7B DD 0B 0B 4F 24 CE BB 1D 24 0D 04 9D 91 5F 5C  {Ý..O$Î».$...'_\
00001890  35 C6 27 7B 6D A0 3F 75 1E 20 89 3A 91 06 DA B7  5Æ'{m ?u. ‰:'.Ú·
000018A0  F6 11 E8 DB 3A AF 04 D4 C1 BB 46 C3 73 34 00 4D  ö.èÛ:¯.ÔÁ»FÃs4.M
000018B0  C1 30 60 BA 74 B4 7D 12 67 87 11 98 82 0C BA F1  Á0`ºt´}.g‡.˜,.ºñ
000018C0  20 B5 A3 CA 4C 72 CC 75 EC 9F C6 54 1A E8 07 EE   µ£ÊLrÌuìŸÆT.è.î
000018D0  9D 82 AB 62 E3 43 13 02 76 E6 51 FD 01 CD D0 A7  .,«bãC..væQý.ÍÐ§
000018E0  F8 44 BA 4C 06 73 13 98 49 68 11 AC 82 01 93 B4  øDºL.s.˜Ih.¬,.“´
000018F0  85 A1 5E 93 09 CA E6 02 4C 36 E0 01 94 58 88 1A  …¡^“.Êæ.L6à.”Xˆ.
00001900  69 61 B4 21 D2 AA 4B 33 C0 F2 8C BA 6E 6E 3F 28  ia´!ÒªK3ÀòŒºnn?(
00001910  0E AB 37 EF DC 58 68 84 E3 B2 AB 1A 19 35 F0 07  .«7ïÜXh„ã²«..5ð.
00001920  05 82 6B 22 C0 91 24 18 CB BC FC A2 D6 B6 A8 55  .,k"À'$.Ë¼ü¢Ö¶¨U
00001930  A9 19 2F 19 46 62 45 B3 4D 8E 9E 50 48 02 6D 3C  ©./.FbE³MŽžPH.m<
00001940  D6 89 3E 68 00 4E 59 FA 5F EE 97 AC 1B 3A 6B 7F  Ö‰>h.NYú_î—¬.:k.
00001950  C7 E1 1E 50 AA 47 FF D9 4D 5A 90 00 03 00 00 00  Çá.PªGÿÙMZ......
00001960  04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00  ....ÿÿ..¸.......
00001970  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @...............
00001980  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001990  00 00 00 00 D8 00 00 00 0E 1F BA 0E 00 B4 09 CD  ....Ø.....º..´.Í
000019A0  21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72  !¸.LÍ!This progr
000019B0  61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E  am cannot be run
000019C0  20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A   in DOS mode....
000019D0  24 00 00 00 00 00 00 00 31 B8 84 3A 75 D9 EA 69  $.......1¸„:uÙêi
000019E0  75 D9 EA 69 75 D9 EA 69 B6 D6 B5 69 77 D9 EA 69  uÙêiuÙêi¶ÖµiwÙêi
000019F0  75 D9 EB 69 EE D9 EA 69 B6 D6 B7 69 64 D9 EA 69  uÙëiîÙêi¶Ö·idÙêi
```

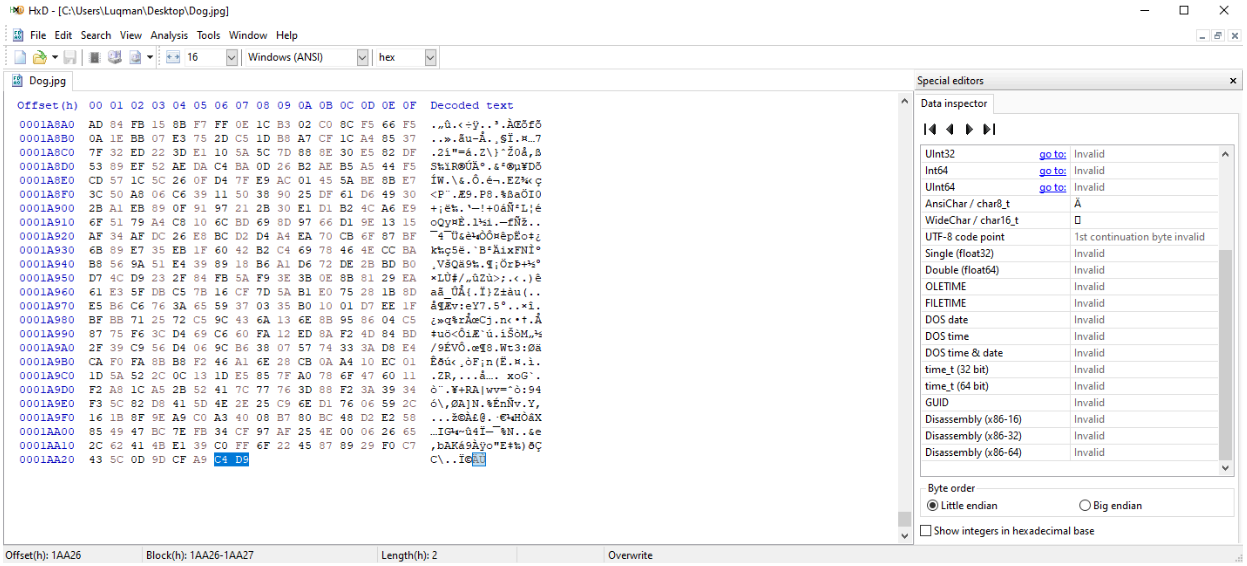
UInt32	go to:	Invalid
Int64	go to:	Invalid
UInt64	go to:	Invalid
AnsiChar / char8_t		ÿ
WideChar / char16_t		▯
UTF-8 code point		Invalid code unit
Single (float32)		Invalid
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		Invalid
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid
time_t (64 bit)		Invalid
GUID		Invalid
Disassembly (x86-16)		Invalid
Disassembly (x86-32)		Invalid
Disassembly (x86-64)		Invalid

Byte order

● Little endian ○ Big endian

□ Show integers in hexadecimal base

Offset(h): 1956 Block(h): 1956-1957 Length(h): 2 Overwrite



HxD - [C:\Users\Luqman\Desktop\Dog.jpg]

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

0001A8A0  AD 84 FB 15 8B F7 FF 0E 1C B3 02 C0 8C F5 66 F5  .„û.‹÷ÿ..³.ÀŒõfõ
0001A8B0  0A 1E BB 07 E3 75 2D C5 1D B8 A7 CF 1C A4 85 37  ..».ãu-Å.¸§Ï.¤…7
0001A8C0  7F 32 ED 22 3D E1 10 5A 5C 7D 88 8E 30 E5 82 DF  .2í"=á.Z\}ˆŽ0å‚ß
0001A8D0  53 89 EF 52 AE DA C4 BA 0D 26 B2 AE B5 A5 44 F5  S‰ïR®ÚÄº.&²®µ¥Dõ
0001A8E0  CD 57 1C 5C 26 0F D4 7F E9 AC 01 45 5A BE 8B E7  ÍW.\&.Ô.é¬.EZ¾‹ç
0001A8F0  3C 50 A8 06 C6 39 11 50 38 90 25 DF 61 D6 49 30  <P¨.Æ9.P8.%ßaÖI0
0001A900  2B A1 EB 89 0F 91 97 21 2B 30 E1 D1 B2 4C A6 E9  +¡ë‰.‘—!+0áÑ²L¦é
0001A910  6F 51 79 A4 C8 10 6C BD 69 8D 97 66 D1 9E 13 15  oQy¤È.l½i.—fÑž..
0001A920  AF 34 AF DC 26 E8 BC D2 D4 A4 EA 70 CB 6F 87 BF  ¯4¯Ü&è¼ÒÔ¤êpËo‡¿
0001A930  6B 89 E7 35 EB 1F 60 42 B2 C4 69 78 46 4E CC BA  k‰ç5ë.`B²ÄixFNÌº
0001A940  B8 56 9A 51 E4 39 89 18 B6 A1 D6 72 DE 2B BD B0  ¸VšQä9‰.¶¡ÖrÞ+½°
0001A950  D7 4C D9 23 2F 84 FB 5A F9 3E 3B 0E 8B 81 29 EA  ×LÙ#/„ûZù>;.‹.)ê
0001A960  61 E3 5F DB C5 7B 16 CF 7D 5A B1 E0 75 28 1B 8D  aã_ÛÅ{.Ï}Z±àu(..
0001A970  E5 B6 C6 76 3A 65 59 37 03 35 B0 10 01 D7 EE 1F  å¶Æv:eY7.5°..×î.
0001A980  BF BB 71 25 72 C5 9C 43 6A 13 6E 8B 95 86 04 C5  ¿»q%rÅœCj.n‹•†.Å
0001A990  87 75 F6 3C D4 69 C6 60 FA 12 ED 8A F2 4D 84 BD  ‡uö<ÔiÆ`ú.íŠòM„½
0001A9A0  2F 39 C9 56 D4 06 9C B6 38 07 57 74 33 3A D8 E4  /9ÉVÔ.œ¶8.Wt3:Øä
0001A9B0  CA F0 FA 8B B8 F2 46 A1 6E 28 CB 0A A4 10 EC 01  Êðú‹¸òF¡n(Ë.¤.ì.
0001A9C0  1D 5A 52 2C 0C 13 1D E5 85 7F A0 78 6F 47 60 11  .ZR,...å…. xoG`.
0001A9D0  F2 A8 1C A5 2B 52 41 7C 77 76 3D 88 F2 3A 39 34  ò¨.¥+RA|wv=ˆò:94
0001A9E0  F3 5C 82 D8 41 5D 4E 2E 25 C9 6E D1 76 06 59 2C  ó\‚ØA]N.%ÉnÑv.Y,
0001A9F0  16 1B 8F 9E A9 C0 A3 40 08 B7 80 BC 48 D2 E2 58  ...ž©À£@.·€¼HÒâX
0001AA00  85 49 47 BC 7E FB 34 CF 97 AF 25 4E 00 06 26 65  …IG¼~û4Ï—¯%N..&e
0001AA10  2C 62 41 4B E1 39 C0 FF 6F 22 45 87 89 29 F0 C7  ,bAKá9Àÿo"E‡‰)ðÇ
0001AA20  43 5C 0D 9D CF A9 C4 D9                          C\..Ï©ÄÙ
```

Offset(h): 1AA26 Block(h): 1AA26-1AA27 Length(h): 2 Overwrite

Special editors

Data inspector

UInt32	go to:	Invalid
Int64	go to:	Invalid
UInt64	go to:	Invalid
AnsiChar / char8_t		Ä
WideChar / char16_t		▯
UTF-8 code point		1st continuation byte invalid
Single (float32)		Invalid
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		Invalid
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid
time_t (64 bit)		Invalid
GUID		Invalid
Disassembly (x86-16)		Invalid
Disassembly (x86-32)		Invalid
Disassembly (x86-64)		Invalid

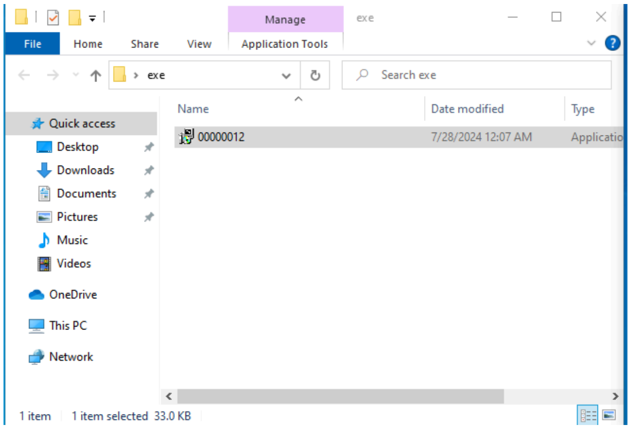
Byte order

● Little endian ○ Big endian

□ Show integers in hexadecimal base

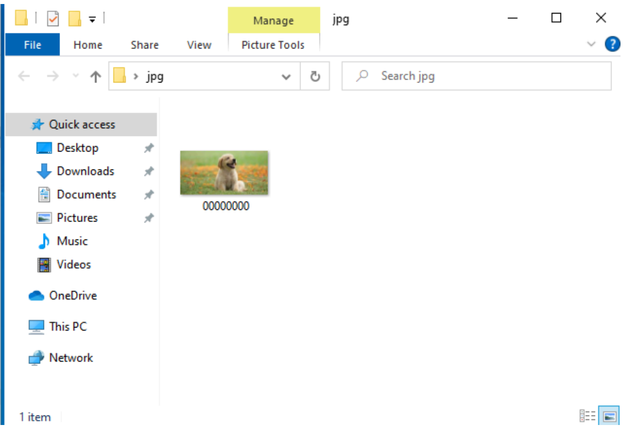
During the investigation, I discovered that an image file contains an embedded executable (EXE) file. This EXE file is identified as the Boaxxe trojan, which is known for its malicious activities such as downloading and installing additional malware, and exfiltrating sensitive data. Immediate actions are required to mitigate the potential threat posed by this embedded malware.

I installed Kali Linux on Windows and used Binwalk to separate the JPG and EXE files.



Name	Date modified	Type
00000012	7/28/2024 12:07 AM	Applicatio

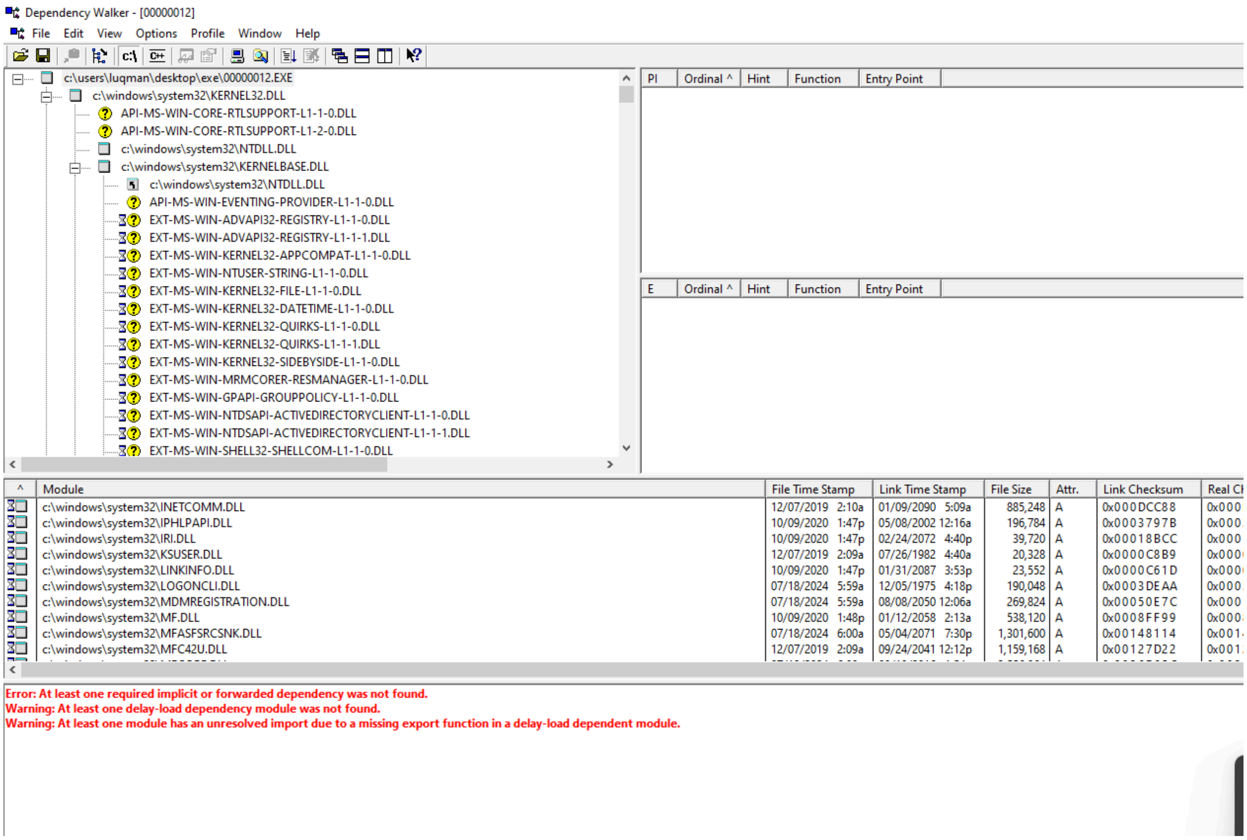
1 item 1 item selected 33.0 KB



00000000

1 item

I extracted sequences of characters that indicate the hidden intentions of the file and its backdoor behavior.

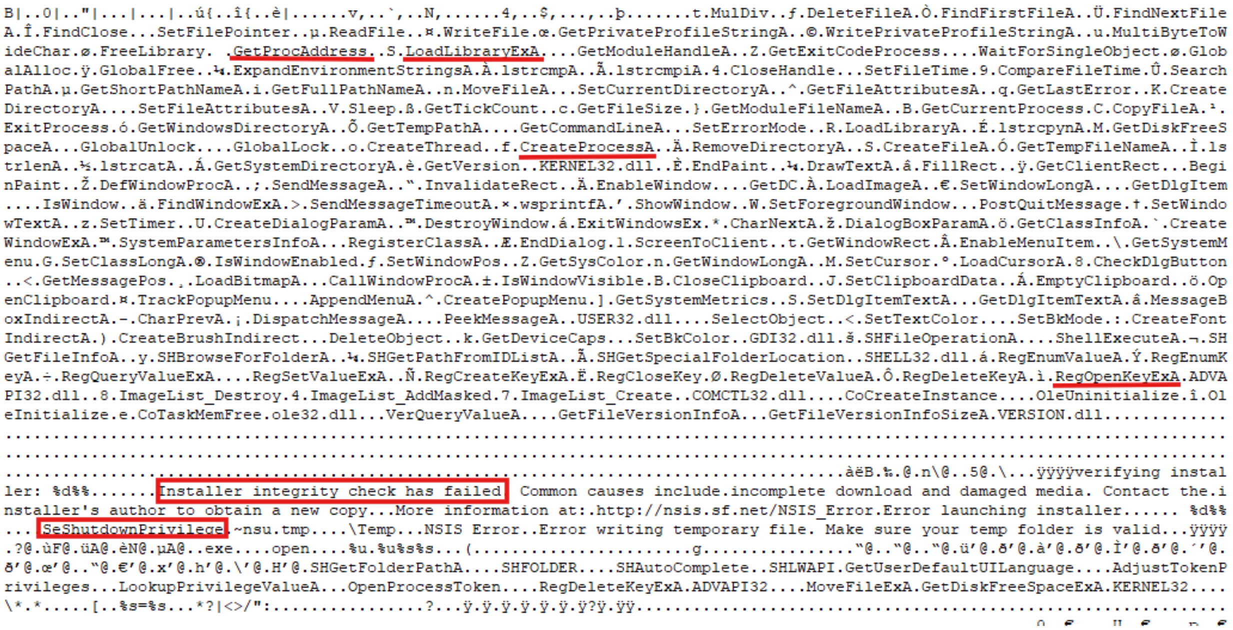


```
c:\users\luqman\desktop\exe\00000012.EXE
    c:\windows\system32\KERNEL32.DLL
        API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
        API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
        c:\windows\system32\NTDLL.DLL
        c:\windows\system32\KERNELBASE.DLL
            c:\windows\system32\NTDLL.DLL
            API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
            EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
            EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
            EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
            EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
            EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
            EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
            EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
            EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
            EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
            EXT-MS-WIN-MRMCORER-RESMANAGER-L1-1-0.DLL
            EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
            EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
            EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL
            EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
```

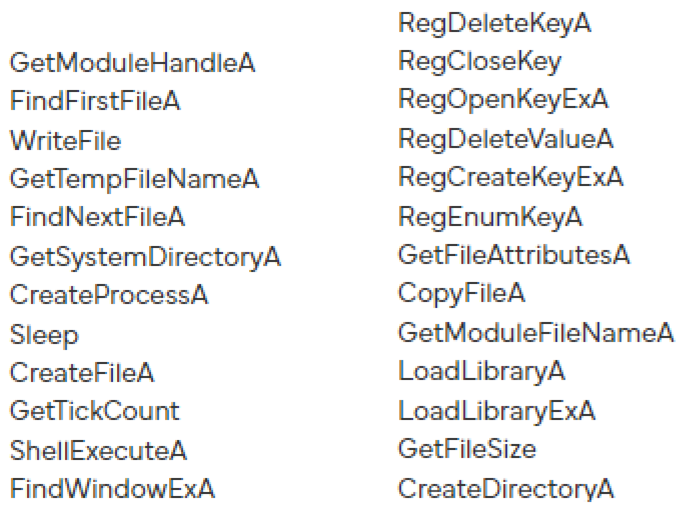
^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Cl
	c:\windows\system32\INETCOMM.DLL	12/07/2019 2:10a	01/09/2090 5:09a	885,248	A	0x000DCC88	0x000
	c:\windows\system32\IPHLPAPI.DLL	10/09/2020 1:47p	05/08/2002 12:16a	196,784	A	0x0003797B	0x000
	c:\windows\system32\IRI.DLL	10/09/2020 1:47p	02/24/2072 4:40p	39,720	A	0x00018BCC	0x000
	c:\windows\system32\KSUSER.DLL	12/07/2019 2:09a	07/26/1982 4:40a	20,328	A	0x0000C8B9	0x000
	c:\windows\system32\LINKINFO.DLL	10/09/2020 1:47p	01/31/2087 3:53p	23,552	A	0x0000C61D	0x000
	c:\windows\system32\LOGONCLI.DLL	07/18/2024 5:59a	12/05/1975 4:18p	190,048	A	0x0003DEAA	0x000
	c:\windows\system32\MDMREGISTRATION.DLL	07/18/2024 5:59a	08/08/2050 12:06a	269,824	A	0x00050E7C	0x000
	c:\windows\system32\MF.DLL	10/09/2020 1:48p	01/12/2058 2:13a	538,120	A	0x0008FF99	0x000
	c:\windows\system32\MFASFSRCSNK.DLL	07/18/2024 6:00a	05/04/2071 7:30p	1,301,600	A	0x00148114	0x001
	c:\windows\system32\MFC42U.DLL	12/07/2019 2:09a	09/24/2041 12:12p	1,159,168	A	0x00127D22	0x001

```
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

Suspicious strings, references, and other sequences of characters indicating that this is malicious software.

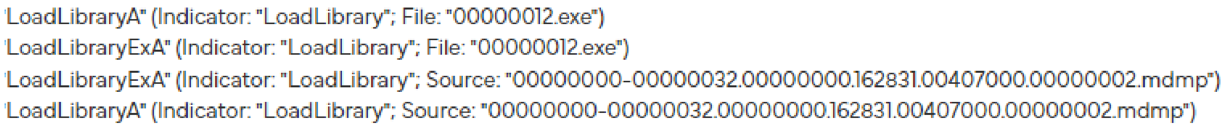


```
B|..0|.."|...|...|..ú{..î{..è|......v,..`,..N,......4,..$,...,..þ.......t.MulDiv..ƒ.DeleteFileA.Ò.FindFirstFileA..Ü.FindNextFile
A.Î.FindClose...SetFilePointer..µ.ReadFile..¤.WriteFile.œ.GetPrivateProfileStringA..©.WritePrivateProfileStringA..u.MultiByteToW
ideChar.ø.FreeLibrary. .GetProcAddress..S.LoadLibraryExA....GetModuleHandleA..Z.GetExitCodeProcess....WaitForSingleObject.ø.Glob
alAlloc.ÿ.GlobalFree..¼.ExpandEnvironmentStringsA.À.lstrcmpA..Ã.lstrcmpiA.4.CloseHandle...SetFileTime.9.CompareFileTime.Û.Search
PathA.µ.GetShortPathNameA.i.GetFullPathNameA..n.MoveFileA...SetCurrentDirectoryA..^.GetFileAttributesA..q.GetLastError..K.Create
DirectoryA....SetFileAttributesA..V.Sleep.ß.GetTickCount..c.GetFileSize.}.GetModuleFileNameA..B.GetCurrentProcess.C.CopyFileA.¹.
ExitProcess.ó.GetWindowsDirectoryA..Õ.GetTempPathA....GetCommandLineA...SetErrorMode..R.LoadLibraryA..É.lstrcpynA.M.GetDiskFreeS
paceA...GlobalUnlock....GlobalLock..o.CreateThread..f.CreateProcessA..Ä.RemoveDirectoryA..S.CreateFileA.Ó.GetTempFileNameA..Ì.ls
trlenA..½.lstrcatA..Á.GetSystemDirectoryA.è.GetVersion..KERNEL32.dll..È.EndPaint..¼.DrawTextA.â.FillRect..ÿ.GetClientRect...Begi
nPaint..Ž.DefWindowProcA..;.SendMessageA..".InvalidateRect..Ä.EnableWindow....GetDC.À.LoadImageA..€.SetWindowLongA....GetDlgItem
....IsWindow..ä.FindWindowExA.>.SendMessageTimeoutA.×.wsprintfA.'.ShowWindow..W.SetForegroundWindow...PostQuitMessage.†.SetWindo
wTextA..z.SetTimer..U.CreateDialogParamA..™.DestroyWindow.á.ExitWindowsEx.*.CharNextA.ž.DialogBoxParamA.ö.GetClassInfoA.`.Create
WindowExA.™.SystemParametersInfoA...RegisterClassA..Æ.EndDialog.l.ScreenToClient..t.GetWindowRect.Â.EnableMenuItem..\.GetSystemM
enu.G.SetClassLongA.®.IsWindowEnabled.ƒ.SetWindowPos..Z.GetSysColor.n.GetWindowLongA..M.SetCursor.°.LoadCursorA.8.CheckDlgButton
..<.GetMessagePos.¸.LoadBitmapA...CallWindowProcA.±.IsWindowVisible.B.CloseClipboard..J.SetClipboardData..Á.EmptyClipboard..ö.Op
enClipboard.¤.TrackPopupMenu....AppendMenuA.^.CreatePopupMenu.].GetSystemMetrics..S.SetDlgItemTextA...GetDlgItemTextA.â.MessageB
oxIndirectA.-.CharPrevA.¡.DispatchMessageA....PeekMessageA..USER32.dll....SelectObject..<.SetTextColor....SetBkMode.:.CreateFont
IndirectA.).CreateBrushIndirect...DeleteObject..k.GetDeviceCaps...SetBkColor..GDI32.dll.š.SHFileOperationA....ShellExecuteA.¬.SH
GetFileInfoA..y.SHBrowseForFolderA..¼.SHGetPathFromIDListA..Ã.SHGetSpecialFolderLocation..SHELL32.dll.á.RegEnumValueA.Ý.RegEnumK
eyA.÷.RegQueryValueExA....RegSetValueExA..Ñ.RegCreateKeyExA.Ë.RegCloseKey.Ø.RegDeleteValueA.Ô.RegDeleteKeyA.ì.RegOpenKeyExA.ADVA
PI32.dll..8.ImageList_Destroy.4.ImageList_AddMasked.7.ImageList_Create..COMCTL32.dll....CoCreateInstance....OleUninitialize.î.Ol
eInitialize.e.CoTaskMemFree.ole32.dll...VerQueryValueA....GetFileVersionInfoA...GetFileVersionInfoSizeA.VERSION.dll............
................................................................................................................................
................................................................................................................................
..........................................................................................àëB.‰.@.n\@..5@.\...ÿÿÿÿverifying instal
ler: %d%%.......Installer integrity check has failed  Common causes include.incomplete download and damaged media. Contact the.i
nstaller's author to obtain a new copy...More information at:.http://nsis.sf.net/NSIS_Error.Error launching installer...... %d%%
... SeShutdownPrivilege.~nsu.tmp....\Temp...NSIS Error..Error writing temporary file. Make sure your temp folder is valid...ÿÿÿÿ
.?@.ùF@.üA@.èN@.µA@..exe....open....%u.%u%s%s...(.........................g................"@.."@.."@.ü'@.ð'@.à'@.ð'@.Ì'@.ð'@.´'@.
ð'@.œ'@.."@.€'@.x'@.h'@.\'@.H'@.SHGetFolderPathA....SHFOLDER....SHAutoComplete..SHLWAPI.GetUserDefaultUILanguage....AdjustTokenP
rivileges...LookupPrivilegeValueA...OpenProcessToken....RegDeleteKeyExA.ADVAPI32....MoveFileExA.GetDiskFreeSpaceExA.KERNEL32....
\*.*.....[..%s=%s...*?|<>/":................?...ÿ.ÿ.ÿ.ÿ.ÿ.ÿ.ÿ?ÿ.ÿÿ..................................................................
```



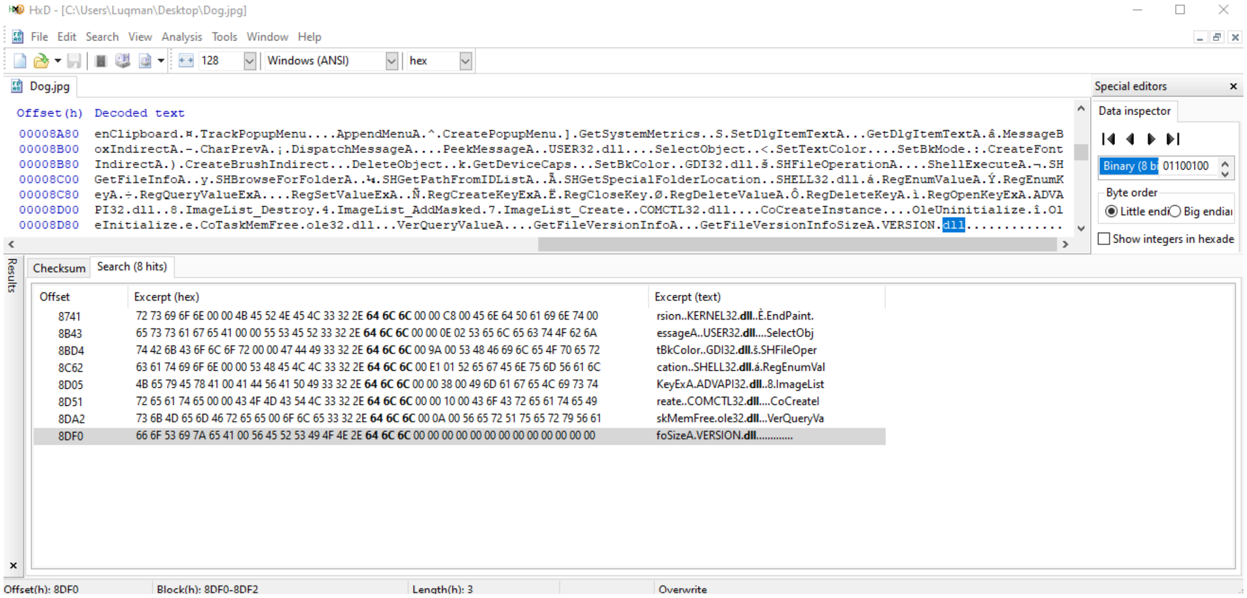
GetModuleHandleA
FindFirstFileA
WriteFile
GetTempFileNameA
FindNextFileA
GetSystemDirectoryA
CreateProcessA
Sleep
CreateFileA
GetTickCount
ShellExecuteA
FindWindowExA

RegDeleteKeyA
RegCloseKey
RegOpenKeyExA
RegDeleteValueA
RegCreateKeyExA
RegEnumKeyA
GetFileAttributesA
CopyFileA
GetModuleFileNameA
LoadLibraryA
LoadLibraryExA
GetFileSize
CreateDirectoryA



'LoadLibraryA" (Indicator: "LoadLibrary"; File: "00000012.exe")
'LoadLibraryExA" (Indicator: "LoadLibrary"; File: "00000012.exe")
'LoadLibraryExA" (Indicator: "LoadLibrary"; Source: "00000000-00000032.00000000.162831.00407000.00000002.mdmp")
'LoadLibraryA" (Indicator: "LoadLibrary"; Source: "00000000-00000032.00000000.162831.00407000.00000002.mdmp")

References to DLL files as well as a nonexistent DLL file.



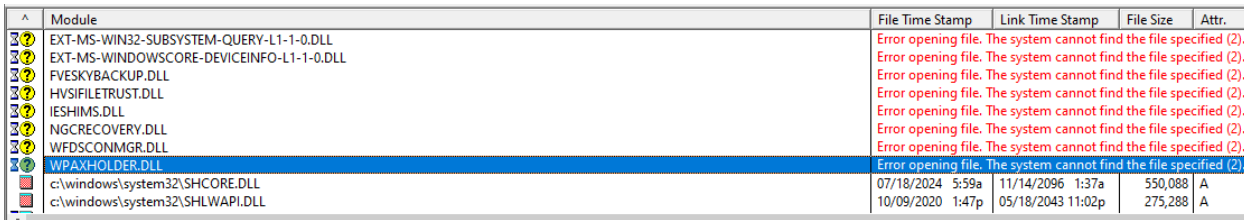
HxD - [C:\Users\Luqman\Desktop\Dog.jpg]
File Edit Search View Analysis Tools Window Help
128
Windows (ANSI)
hex
Dog.jpg
Special editors
Data inspector
Binary (8 bi 01100100
Byte order
● Little endi ○ Big endiai
□ Show integers in hexade
Results
Checksum
Search (8 hits)

```
Offset(h) Decoded text
00008A80  enClipboard.¤.TrackPopupMenu....AppendMenuA.^.CreatePopupMenu.].GetSystemMetrics..S.SetDlgItemTextA...GetDlgItemTextA.â.MessageB
00008B00  oxIndirectA.–.CharPrevA.¡.DispatchMessageA....PeekMessageA..USER32.dll....SelectObject..<.SetTextColor....SetBkMode.:.CreateFont
00008B80  IndirectA.).CreateBrushIndirect...DeleteObject..k.GetDeviceCaps...SetBkColor..GDI32.dll.š.SHFileOperationA....ShellExecuteA.¬.SH
00008C00  GetFileInfoA..y.SHBrowseForFolderA..¼.SHGetPathFromIDListA..Ã.SHGetSpecialFolderLocation..SHELL32.dll.á.RegEnumValueA.Ý.RegEnumK
00008C80  eyA.÷.RegQueryValueExA....RegSetValueExA..Ñ.RegCreateKeyExA.Ë.RegCloseKey.Ø.RegDeleteValueA.Ô.RegDeleteKeyA.ì.RegOpenKeyExA.ADVA
00008D00  PI32.dll..8.ImageList_Destroy.4.ImageList_AddMasked.7.ImageList_Create..COMCTL32.dll....CoCreateInstance....OleUninitialize.î.Ol
00008D80  eInitialize.e.CoTaskMemFree.ole32.dll...VerQueryValueA....GetFileVersionInfoA...GetFileVersionInfoSizeA.VERSION.dll............
```

Offset	Excerpt (hex)	Excerpt (text)
8741	72 73 69 6F 6E 00 00 4B 45 52 4E 45 4C 33 32 2E **64 6C 6C** 00 00 C8 00 45 6E 64 50 61 69 6E 74 00	rsion..KERNEL32.**dll**..È.EndPaint.
8B43	65 73 73 61 67 65 41 00 00 55 53 45 52 33 32 2E **64 6C 6C** 00 00 0E 02 53 65 6C 65 63 74 4F 62 6A	essageA..USER32.**dll**....SelectObj
8BD4	74 42 6B 43 6F 6C 6F 72 00 00 47 44 49 33 32 2E **64 6C 6C** 00 9A 00 53 48 46 69 6C 65 4F 70 65 72	tBkColor..GDI32.**dll**.š.SHFileOper
8C62	63 61 74 69 6F 6E 00 00 53 48 45 4C 4C 33 32 2E **64 6C 6C** 00 E1 01 52 65 67 45 6E 75 6D 56 61 6C	cation..SHELL32.**dll**.á.RegEnumVal
8D05	4B 65 79 45 78 41 00 41 44 56 41 50 49 33 32 2E **64 6C 6C** 00 00 38 00 49 6D 61 67 65 4C 69 73 74	KeyExA.ADVAPI32.**dll**..8.ImageList
8D51	72 65 61 74 65 00 00 43 4F 4D 43 54 4C 33 32 2E **64 6C 6C** 00 00 10 00 43 6F 43 72 65 61 74 65 49	reate..COMCTL32.**dll**....CoCreateI
8DA2	73 6B 4D 65 6D 46 72 65 65 00 6F 6C 65 33 32 2E **64 6C 6C** 00 0A 00 56 65 72 51 75 65 72 79 56 61	skMemFree.ole32.**dll**...VerQueryVa
8DF0	66 6F 53 69 7A 65 41 00 56 45 52 53 49 4F 4E 2E **64 6C 6C** 00 00 00 00 00 00 00 00 00 00 00 00 00	foSizeA.VERSION.**dll**............

Offset(h): 8DF0 Block(h): 8DF0-8DF2 Length(h): 3 Overwrite

Nonexistent dll



^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.
⌛?	EXT-MS-WIN32-SUBSYSTEM-QUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	EXT-MS-WINDOWSCORE-DEVICEINFO-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	FVESKYBACKUP.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	HVSIFILETRUST.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	NGCRECOVERY.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	WFDSCONMGR.DLL	Error opening file. The system cannot find the file specified (2).			
⌛?	WPAXHOLDER.DLL	Error opening file. The system cannot find the file specified (2).			
▨	c:\windows\system32\SHCORE.DLL	07/18/2024 5:59a	11/14/2096 1:37a	550,088	A
▨	c:\windows\system32\SHLWAPI.DLL	10/09/2020 1:47p	05/18/2043 11:02p	275,288	A

In summary, the JPG file contained an embedded EXE file that references Windows libraries and includes potentially malicious software. This software attempts to install itself, create files, and run at system startup. The embedded EXE has been identified as Boaxxe, a trojan known for downloading additional malware and exfiltrating sensitive data.